ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR COUPLING AN X.509 DIGITAL CERTIFICATE WITH A HOST IDENTITY

A method or system is presented for coupling identities through the use of digital certificates, thereby allowing a client to be authenticated for a variety of services without those services having to modify their existing methods of authentication. The client generates a request for a digital certificate containing its host identity for a targeted host and secret data associated with its host identity. The secret data has been encrypted using the public key of the certifying authority that receives the request for the digital certificate. The certifying authority decrypts the secret data using its private key and encrypts the secret data using the public key of the targeted host. The digital certificate is then generated and returned to the client. At some point in time, a host receives the certificate from the client and obtains the client's host identity from the certificate, i.e. the host identity uniquely identifies the client or the user of the client to the host. Encrypted secret data associated with the host identity, such as a password, is also retrieved from the digital certificate. The host decrypts the secret data with its private key, and the host then authenticates the client using the host identity and the decrypted secret data for various services. The digital certificate may be formatted according to the X.509 standard, and the host identity and secret information may be stored in an X.509 extension within the digital certificate.